REMARKS

I. Status of the Claims

Original claims 1-5 and new claims 6-7 are the only claims pending in this application.

II. Rejections Based On Prior Art

The Office Action rejects claims 1 under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 5,003,598 ("Kunstadt") in view of M. Rabin, Department of Mathematics, The Hebrew University of Jerusalem, Jerusalem, Israel, "Transaction Protection by Beacons," Journal of Computer and System Sciences 27, 256-267 (1983) ("Rabin").

A. The Combined Teachings of Kunstadt and Rabin Fail to Establish *Prima Facie* Obviousness of Base Claim 1.

Applicant respectfully submits that the collected teachings of Kunstadt and Rabin do not teach, disclose or suggest any system, method or apparatus within the broadest reasonable meaning of claim 1.

Kunstadt lacks the limitation of broadcasting a random number sequence. Rabin lacks any teaching or suggestion to modifying Kunstadt to have this limitation, and such a modification would destroy Kunstadt's principle of operation and render it useless for its intended purpose. Further, the combined teachings of Kunstadt and Rabin lack any disclosure, teaching or suggestion of selecting, at the transmitter, a subsequence from the publicly broadcast sequence based on a private key, encrypting data based on the selected subsequence. Still further, the combined teachings of Kunstadt and Rabin lack any disclosure, teaching or suggestion of selecting, at the receiver, a subsequence from the publicly broadcast sequence based on a private key, decrypting the data based on the selected subsequence.

Applicant therefore respectfully urges that the rejection of base claim 1 be withdrawn.

1. Kunstadt Lacks the Claim 1 Limitation of Transmitting a Random Sequence.

Applicant's claim 1 recites, among other limitations:

> generating a random number sequence,
>
> transmitting the random number sequence to a data encryption station and a data decryption station

Claim 1 at lines 3-5.

The Office Action states that Kunstadt "is silent on using the unrelated publicly available broadcast station to transmit [a] random number." Office Action at ¶ 5.

Applicant respectfully submits that the Office Action's statement that Kunstadt is silent on using a "publicly available broadcast station to transmit a random number" substantially mischaracterizes that reference. Kunstadt discloses the exact opposite of a public transmission of a random number sequence; it absolutely relies on the same <u>private</u> random number sequence being generated at each of the transmitter and the receiver, with absolutely no generation or transmission, explicitly or inherently, of <u>any</u> <u>public</u> random number. The transmitting station and the receiving station generates exactly the same private random number sequence by each having the same configuration of random number generator, with each generator having its initialization data switches set to exactly the same value. Further, it is crucial to Kunstadt's method that the sender <u>locally</u> generates a <u>private</u> random number sequence, and that the receiver <u>locally</u> generates the <u>same</u> private random number sequence, and that there be <u>no</u> public communication, <u>whatsoever</u>, of that sequence.

2. Kunstadt Cannot Be Modified to Include Transmitting a Random Number Sequence Without Both Radically Changing Its Principle of Operation and Making It Unfit for Its Intended Purpose.

The Office Action states that Rabin provides the necessary teaching such that "one of ordinary skill in the art at the time the invention was made would have been motivated to combine" their respective teachings to have the limitations of "generating a random number sequence," and "transmitting the random number sequence to a data encryption station and a data decryption station." Office Action at ¶¶ 4-5.

Applicant again respectfully submits that the statement that Kunstadt is silent on using a "publicly available broadcast station to transmit a random number" is a mischaracterization of that reference. Changing Kunstadt's method to employ a publicly transmitted random number would require a total redesign of the system, its architecture, and its principle of operation.

More particularly, Kunstadt discloses a sending location 30 and a receiving location 31, with both the sending location and the receiving location having a random number generator. Circuitry at the sending location detects the beginning of a spoken word and resets its random number generator 49 to a preset starting position, namely that of switches 53. *See* Kunstadt at column 3, lines 19-31. The locally generated random number sequence is input to a D/A converter to generate a noise signal, and the noise signal is mixed with the spoken word and transmitted to the receiving location. The receiving location has the same random number generator as the sending location, and its switches 53 are set to the same preloaded starting position. Since the receiving location's random number generator is identical to the sender's number generator, and both have their switches set to the same starting value, the receiving location locally generates the exact same sequence as that which was generated locally by the sending location to encrypt the signal. *See* Kunstadt at column 3, lines 27-31 and lines 59-63. This number sequence locally generated at the receiving location is input to its D/A converter and mixed with, or subtracted from, the received signal, to obtain the original spoken word. *Id.*

The only information or signal that is "publicly broadcast" by Kunstadt's disclosed method is the sending location's transmitted voice signal, after being mixed with the random noise. The random signal itself is not publicly broadcast. It cannot be because, if it were, anyone receiving the signal could decrypt it, if the sequence generated by 49 were "publicly broadcast" then <u>any</u> party receiving the transmission could decrypt the signal. For the same reason, the random sequence generated by the sending location <u>cannot</u> be recovered from the mixed signal transmitted by the sending location, by anyone unless the receiving party has a complete, and infinitely accurate, *a priori* knowledge of the spoken words that are "encrypted" within the mixed signal. That would not be a "receiver" within its understood meaning.

3. Kunstadt Lacks the Claim 1 Limitations of Selecting a Data Encryption Subsequence at the Encryption Station and Selecting a Data Subsequence at the Decryption Station.

Applicant's claim 1 further recites:

generating a private key;

inputting the private key to the data encryption station and to the data decryption station;

selecting at the data encryption station an encryption subsequence from the random number sequence, the boundaries of the encryption subsequence based on the private key

Claim 1 at lines 6-11.

The Office Action does not state that the above-quoted claim 1 language is disclosed by Kunstadt. The Office Action instead states that

> [t]he limitation of extracting keying material use[d] for encryption and decryption of messages from a[n] unrelated publicly available broadcast station being readily and reliably available at both sending (encryption station) and receiving (decryption station) is taught [by Kunstadt].

Office Action at ¶ 5.

Applicant respectfully submits that the above-quoted subject matter identified by the Office Action as disclosed by Kunstadt does not, in fact, exist within that reference. Neither the Abstract nor the remainder of the Kunstadt reference teaches anything that relates to, much less that is within the broadest reasonable meaning of, the limitation "selecting an encryption subsequence...based on the private key" recited by claim 1.

Kunstadt does not disclose, teach or suggest "extracting keying material use[d] for encryption or decryption" from any publicly broadcast information.

Kunstadt uses the term "keying signals" to mean pulses that reset the local random number generators, not to mean a "key" that is used to encrypt and decrypt data, as that term is normally used in the encryption arts. Kunstadt's resetting, or "keying" pulses are not a private information; they are a trigger based on the beginning of a spoken word, or the beginning of a noise-encrypted utterance, which is detectable by any recipient, intended or unintended. More particularly, Kunstadt uses the term "keying signal" in reference to the sending location's detection of a spoken word, which resets the sender's local random number generator 49 with the switch 53 value, and the receiving location's detection of the beginning of received noise burst, which resets its local random number generator 49 with the same switch 53 values. Kunstadt's method does not extract any keying information used for encryption, or decryption from anything. The only "keying information" that Kunstadt discloses is the setting of the switches 53. The setting of the switches 53 is <u>not</u> extracted from any publicly broadcast information.

The Office Action states that "[t]he limitation of selecting a portion of the publicly available broadcast station based upon predetermined secret information (applicant's private key) is disclosed by Kunstadt in the Abstract." Office Action at ¶ 5.

Kunstadt has no such disclosure. Kunstadt does not select any portion of the signal transmitted by the sending location based on anything, much less based on a predetermined secret information.

Kunstadt's method uses the switch 53 preload for the sending location's random number generator and a copy of the same switch 53 for the receiving location's random number generator. The switch 53 value at both the sending location and the receiving location is roughly comparable to a "private key." That fact does not make Kunstadt into a disclosure of "selecting at the data encryption station an encryption subsequence from the random number sequence, the boundaries of the encryption subsequence based on the private key." It cannot because Kunstadt does not perform, or describe or suggest anything of these claim 1 selecting acts.

First, Kunstadt does not generate a random number sequence and transmit that sequence to the sending location (or to the receiving location). Kunstadt cannot disclose, or suggest selecting from that which it does not have.

Second, Kunstadt discloses that each time the sending location detects the beginning of a word, and the receiving location detects the beginning of a noise burst, each resets its local random number to the same switch 53 preload. That resetting to the switch 53 preload is not within the broadest reasonable meaning of "selecting at the data encryption station an encryption subsequence from the random number sequence."

Third is that Kunstadt does not teach, disclose or suggest anything of selecting the boundaries of the encryption subsequence from a random number sequence, based on anything, much less a selecting based on a private key.

4. Rabin Does Not Teach or Suggest Modifying Kunstadt to Have the Claim 1 Limitations of Transmitting a Random Number Sequence, or of Selecting a Subsequence from a Transmitted Random Number Sequence.

Rabin discloses a protocol that piggybacks on a standard public key encryption system and which purportedly reduces the probability of cheating in the execution of contracts, and in the reception and execution of non-disclosure agreements. Rabin, to the extent it can be understood, employs a protocol that transmits K public keys, with a time-stamp, and a requirement that a designated receiver use one of the K public keys, which is that receiver's public key, to sign and return a contract before expiration of a designated time period.

Rabin's protocol does not include, employ, or suggest the broadcast of a random number sequence that is received by a transmitting station and a receiving station, the transmitting station selecting a subsequence from that received random number sequence, the boundaries of the subsequence based on a private key, and then encrypting a message using the selected subsequence.

Rabin's protocol does not include, employ, or suggest a receiving station receiving an encrypted message, the receiving station selected the same subsequence from the broadcast random number sequence, the selection based on a private key, and then using that selected subsequence to decrypt a message.

In addition to lacking the above-identified limitations of Applicant's claim 1, Rabin states nothing that motivates or suggests to one of ordinary skill reworking Kunstadt to employ a publicly broadcast random number sequence. Further, as Applicant has respectfully submitted at subparagraph 2 hereinabove, such a modification, if suggested by any reference, and no references of record have such a suggestion, would radically change Kunstadt's principle of operation.

B. The Collected Teachings of Kunstadt, Rabin and Maurer Lack the Requirements for Establishing Prima Facie Obviousness of Base Claim 1, or any of its Dependent Claims.

The originally filed claims 2-5 stand rejected as being obvious under 35 U.S.C. § 103 over Kunstadt, Rabin and U.S. Patent No. 5,161,244 ("Maurer"). Office Action at ¶¶ 7-11. Applicant respectfully submits that the collected teachings of Kunstadt, Rabin and Maurer fail to establish prima facie obviousness of base claim 1, or any of its dependent claims 2-5.

A threshold requirement for establishing obviousness of any of the dependent claims 2-5 is that the references establish obviousness of base claim 1. Kunstadt and Rabin, taken in any order, fail to establish prima facie obviousness of base claim 1. Maurer adds nothing to Kunstadt and Rabin that is in the direction of Applicant's claimed invention.

Before addressing Maurer, Applicant respectfully responds to the Office Action's statements regarding that "[t]he limitation of selecting a portion of the public[ly] available broadcast station based upon predetermined secret information (applicant's private key) is disclosed by Kunstadt in the Abstract." Office Action at ¶ 8. Kunstadt teaches nothing of selecting a portion of a publicly broadcast random number sequence, based on anything, much less based on a private key. Kunstadt does not broadcast a random number sequence. Kunstadt does not receive a random number sequence. Kunstadt transmits data encrypted by noise, the noise being based on a private random number sequence generated by the transmitter. The generated random number sequence, however, is categorically non-extractable from the transmitted encrypted data. If it were extractable the encryption would be useless. Kunstadt discloses that the data is decrypted by the receiver generating the exact same private random number sequence that was generated by the transmitter. In Kunstadt's method, the transmitter and the receiver are able to generate the same private random number sequence because the random number generator of each is preloaded with the same private initialization key. However, there is no public broadcast of a random number sequence, and there is no selection of a portion of a broadcast random number sequence.

Maurer teaches nothing of broadcasting a random number sequence to a transmitter and a receiver. Maurer teaches encrypting data at one site, transmitting the encrypted data to a second site, and decrypting it. The transmitting site and the receiving site each generates the same private random number sequence, which the transmitting site uses to encrypt the data, and which the receiving site uses to encrypt it. The random number sequence generated by the transmitting site is not, and cannot, be extractable from the transmitted encrypted data. Maurer discloses nothing of selecting a portion of a publicly broadcast random number sequence, based on anything, much less based on a private key. Maurer discloses nothing of encrypting or decrypting data based on a publicly broadcast random number sequence, or on a selected portion of a publicly broadcast random number sequence.

The collected teachings of Kunstadt, Rabin and Maurer therefore lack the requirements for establishing prima facie obviousness of base claim 1. Claims 2 through 5 are therefore patentable for this reason alone.

Further, with respect to claim 2, the Office Action states that Maurer discloses the storage of random number strings for later use in both sites. Office Action at ¶ 9. Maurer indeed discloses storage at site A and site B for storing respective strings of data. Maurer teaches nothing of broadcasting a random number sequence. Maurer teaches nothing of selecting a portion of a broadcast random number sequence, based on anything, and certainly not according to boundaries based on any private key. The only disclose that Maurer contains is a memory resource at the transmitter and the receiver, for storing information that the respective sites use in their encryption and decryption of data. Neither Applicant's claim 1 nor any of its dependent claims 2-5 are directed to memory resources. Most transmitters and most receivers have memory resources. Maurer adds nothing to modify the collected teachings of Kunstadt and Rabin anywhere toward Applicant's base 1, and/or anywhere toward the added limitations of its dependent claim 2.

With respect to claim 3, the Office Action asserts that since Maurer's memory resources have finite capacity the limitations of the claim are inherently disclose. Office Action at ¶ 10. The Office Action fails to consider all of the limitations of claim 3. Claim 3 recites "sampling the random number sequence at the encryption station for a predetermined interval beginning at a time based on t, to generate a sampled block of bits." Claim 3 at lines 6-8. The collected teachings of Kunstadt, Rabin and Maurer teach nothing of this operation. Therefore, the collected teachings of Kunstadt, Rabin and Maurer teach nothing showing that the contents of the memory resources of Maurer ever contained information selected from a publicly broadcast random number sequence. Maurer therefore does not disclose the claim 3 operations of "detecting a number of bits in said random number reservoir," or "comparing the number of bits detected by said detecting step with a predetermined reservoir full value," or "based on said comparing detecting the number of bits in said random number reservoir being less than said predetermined reservoir full value, performing a step of storing the sampled block of bits in a random number reservoir."

With respect to claim 4, Applicant respectfully submits that the collected teachings of Kunstadt, Rabin and Maurer do not disclose anything of any private key used for selecting a portion of a publicly broadcast random number sequence. Claims 4 and 1 together recite a private key performing recited operations and functions. The collected teachings of Kunstadt, Rabin and Maurer do not disclose Applicant's claimed private key, or generating another of such recited private keys.

C. New Claims 6 and 7 are Patentable Over the Collected Teachings of Kunstadt, Rabin and Maurer.

New claim 6 recites, *inter alia*, generating a random number sequence, receiving the random number sequence at a transmitter station, selecting a portion of the received random number sequence based on a private key, and using the selected portion to encrypt a data. As Applicant presents above, the collected teachings of Kunstadt, Rabin and Maurer disclose nothing of this recited combination of operations.

New claim 7, dependent from claim 6, recites, *inter alia*, generating a random number sequence, receiving the random number sequence at a receiving station, selecting a portion of the received random number sequence based on a private key, and using the selected portion to decrypt data, the data encrypted as recited by claim 6. As Applicant presents above, the collected teachings of Kunstadt, Rabin and Maurer disclose nothing of this recited combination of operations.

III. Conclusion

Applicant respectfully submits, for the reasons presented above, that all pending claims of the present application stand in condition for allowance.

The Examiner is respectfully requested to contact the undersigned, at the telephone number below, if any further action or changes are deemed necessary to expedite this case.

Respectfully submitted,

By ______________________ Date: 12|5|2003

Laurence E. Stein,
Reg. No. 35,371
PATTON BOGGS LLP
2550 M Street, N.W.
Washington, D.C. 20037
202-457-6491 (direct)